Derwent Record

Derwent Title: **Vehicle anti-false microwave electronic card, detection system and method**

Original Title: ☑ CN1367465A: VEHICLE ANTIFALSE WICROWAVE ELECTRONIC CARD, DETECTION SYSTEM AND METHOD

Assignee: **QIAO Y** Individual

Inventor: **QIAO Y;**

Accession/ Update: **2003-041764 / 200304**

IPC Code: **G06K 19/073 ;**

Derwent Classes: **T04**; **T07**; **W02**;

Manual Codes: **T04-K02**(Reading and writing aspects) , **T07-A03A** (Transponder interrogation) , **W02-G05**(Transponder, responder, repeater)

Derwent Abstract: (CN1367465A) **Novelty** - The present invention discloses an anti-false microwave electronic card for vehicle, detection system and method. The microwave electronic card includes processor CPU, read-only memory ROM, microwave transmitter, microwave receiver, weak-up timer and identifier recognition area, in which the basic information of vehicle can be written. The detection system includes reading/writing detection unit and quick search auxiliary unit, and can utilize microwave to make non-contract reading and writing of the microwave electronic card. Its detection method is to utilize the 'fixed or mobile (hand held type) detection mode' of detection system to read out data stored on the microwave electronic card on the vehicle so as to recognize vehicle and distinguish the true from the false.

Dwg.0/0

Family:

PDF	Patent	Pub. Date	Derwent Update	Pages	Language	IPC Code
☑	CN1367465A	* 2002-09-04	200304		English	G06K 19/073

Local appls.: CN2001000102257 Filed:2001-01-20 (2001CN-0102257)

Priority Number:

Application Number	Filed	Original Title
CN2001000102257	2001-01-20	VEHICLE ANTIFALSE WICROWAVE ELECTRONIC CARD, DETECTION SYSTEM AND METHOD

Title Terms: VEHICLE ANTI FALSE MICROWAVE ELECTRONIC CARD DETECT SYSTEM METHOD

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06K 19/073

[12]发明专利申请公开说明书

[21]申请号 01102257.4

[43]公开日 2002年9月4日

[11]公开号 CN 1367465A

[22]申请日 2001.1.20 [21]申请号 01102257.4

[71]申请人 乔永康

地址 030002 山西省太原市迎泽区韶九巷10号省税务局宿舍4楼1单元3号

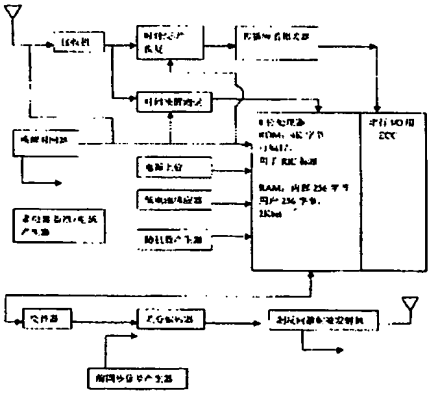
[72]发明人 乔永康

权利要求书3页 说明书18页 附图页数6页

[54]发明名称 机动车防伪微波电子卡、检测系统及方法

[57]摘要

本发明公开一种车辆防伪微波电子卡、检测系统及方法。微波电子卡包括有处理器CPU、只读存储器ROM、动态存储器RAM、微波发射机、微波接收机、唤醒时间器、标识符识别区，其中写入车辆的基本信息。检测系统包括读写检测单元、快速检索辅助单元，通过微波对微波电子卡进行非接触式读写。所述检测方法就是利用检测系统<固定或移动(手持式)检测方式>；读出车辆上的微波电子卡所存储的数据，以此对车辆进行鉴别，以判定车辆的真伪。



ISSN1008-4274

知识产权出版社出版

权 利 要 求 书

1、 一种车辆防伪微波电子卡，其特征是：它包括有微处理器 CPU、只读存储器 ROM、动态存储器 RAM、微波发射机、微波接收机、唤醒时间器、标识符识别区；每一个微波电子卡的标识符识别区中有一个芯片的出厂唯一编号；所述动态存储器 RAM 中存储有下述各种代码：<车辆国际终身编码>、<车主身份证号>、<车牌号>、<发动机号>、<车架号>、<车型>、<识别代码>；所述只读存储器 ROM 中存储有芯片管理系统 COS，即监控程序，管理上述动态存储器 RAM 中的信息的读或不能读、写或不能写、改或不能改；微波发射机、接收机用于与外界设备进行连接，向微波电子卡中写入数据或读出微波电子卡中的数据；唤醒时间器用于控制微波电子卡的“休眠”与工作状态转换；微波发射机、接收机所用的频率为下述三个频段之一：900~928MHZ、2.45GHZ、5.8GHZ。

2、 如权利要求 1 所述的车辆防伪微波电子卡，其特征是：微波电子卡内设置有数据自毁终端，在遇破坏或被强行取走时，存储数据自动消失。

3、 一种车辆防伪微波电子卡检测系统，包括读写检测单元、快速检索辅助单元；其中读写检测单元用于向防伪微波电子卡发送数据并接收来自防伪微波电子卡的应答信号，它包括数字电路模快、射频电路模块和天线；数字电路模块又包括控制部分和数据解调部分，射频电路模块调制发射到防伪微波电子卡的数据，提供一个连续载波用于防伪微波电子卡的反向散射波，接收和解调来自防伪微波电子卡的反向散射波信

号；快速检索辅助单元主要由单片机 MCU 组成，它与读写检测单元相连，对读写检测单元读入的数据进行分析处理；射频电路模块所用的频率为下述三个频段之一：900~928MHZ、2.45GHZ、5.8GHZ。

4、 如权利要求 3 所述的车辆防伪微波电子卡检测系统，其特征是：还包括有系统微机，它与读写检测单元的连接是通过快速检索辅助单元，它与快速检索辅助单元中的单片机 MCU 之间采用高速双口 RAM 以并行方式传送数据，并可以采集、存储、比对、分析、处理车辆微波电子卡内的有关信息；它还通过网络连接公安部交管局各省、市车辆管理所的局域网上，上传、存放、下载各种车辆专用信息；其中还设有疑点车辆数据库；可以按检测结果发出截停或放行车辆的指令。

5、 如权利要求 3 或 4 所述的车辆防伪微波电子卡检测系统，其特征是：所述检测系统是固定式；还设置有数字式车辆检测器、自动道闸和电子眼；数字式车辆检测器采用数模转化技术，通过电磁感应原理，感应检测并计数通行车辆；自动道闸用于拦截疑点车辆；电子眼用于对车辆进行摄像，它包括抓拍系统的图像获得、图像识别、图像存储、图像处理技术。

6、 如权利要求 3 或 4 所述的车辆防伪微波电子卡检测系统，其特征是：所述检测系统为移动式(包括手持式)，所述微机为手提式电脑，通过无线调制解调器上网传输数据。

7、 一种利用权利要求 1 所述车辆防伪微波电子卡和权利要求 3 所述车辆防伪微波电子卡检测系统进行车辆防伪的方法，其特征是包括以下步骤：1）将微波电子卡初识化及个人化，包括由交管部门向车辆防伪微波电子卡中写入下述几种信息：车辆国际终身编码、车主身份证号、车牌号、发动机号、车架号、车型、识别代码；2）初始化及个人化的微波电子卡连同车牌一起发给车主，作为车辆入户认证的电子身份证；3）将微波电子卡安装于车辆前挡风玻璃。

8、 如权利要求 7 所述的车辆防伪方法，其特征是：在对微波电子卡进行初始化及个人化时，还将下述几种信息的至少二种进行押码加密处理，然后将加密后的信息一并写入微波电子卡中：<车辆国际终身编码>、<车主身份证号>、<车牌号>皆须进行押码处理；发动机号、车架号、车型、识别代码不用进行押码处理。

9、 如权利要求 7 或 8 所述的车辆防伪方法，其特征是：在主干道、检查站、道桥关口等处设置固定式车辆防伪微波电子卡检测系统，在不停车的情况下对过往车辆进行逐一检查或随机检查；快速检索辅助单元通过检测单元利用微波信号即时读取被检车辆上的微波电子卡内的数据，传送到系统微机，系统微机对数据进行处理，决定放行或截停车辆。

10、 如权利要求 7 或 8 所述的车辆防伪方法，其特征是：在巡查车上设置移动式车辆防伪微波电子卡检测系统，对过往车辆进行人机相结合的随机检查，快速检索辅助单元通过检测单元利用微波信号即时读取被检车辆上的微波电子卡内的数据，传送到系统微机，系统微机对数据进行处理，决定放行或截停车辆。

11、 如权利要求 7 或 8 所述的车辆防伪方法，其特征是：执勤者持手持式车辆防伪微波电子卡检测系统，对过往车辆或停泊车辆进行人机相结合的随机检查，快速检索检测系统<疑点车辆数据库>，决定放行或截停、扣押车辆。

说 明 书

机动车防伪微波电子卡、检测系统及方法

本发明涉及一种车辆防伪系统及方法，特别是利用微波电子卡实现车辆防伪的系统及方法。

机动车被盗抢问题是现今社会的一大难题。现在对机动车的通行管理方法是利用车牌号进行管理。但车牌号极易伪造，这给盗车、抢劫、销赃、黑市交易带来了可乘之机。显然，如果能够给每一辆车一个唯一的、不可伪造的、且易于识别的编号作为其“身份证明”，上述非法活动肯定会被大大抑制。但现在的各种编号，包括车架号、发动机号等都无法满足这一要求，因为它们有的不易识别，有的容易伪造。

本发明的目的就是为了解决以上问题，提供一种车辆防伪微波电子卡、检测系统，以及利用这种微波电子卡和检测系统的车辆防伪方法，使检查方便、可靠。

本发明实现上述目的的方案包括一种车辆防伪微波电子卡、微波电子卡检测系统及基于此微波电子卡和检测系统的车辆防伪检测方法。

所述车辆防伪微波电子卡的其特征是：它包括有处理器 CPU、只读存储器 ROM、动态存储器 RAM、微波发射机、微波接收机、唤醒时间器、标识符识别区；每一个微波电子卡的标识符识别区中有一个芯片的出厂唯一编号；所述动态存储器 RAM 中存储有下述各种代码：<车辆国际终身编码>、<车主身份证号>、<车牌号>、<发动机号>、<车架号>、<车型>、<识别代码>；所述只读存储器 ROM 中存储有芯片管理系统 COS，

即监控程序，管理上述动态存储器 RAM 中的信息的读或不能读、写或不能写、改或不能改；微波发射机、接收机用于与外界设备进行连接，向微波电子卡中写入数据或读出微波电子卡中的数据；唤醒时间器用于控制微波电子卡的“休眠”与工作状态转换。

所述车辆防伪微波电子卡检测系统包括读写检测单元、快速检索辅助单元；其中读写检测单元用于向防伪微波电子卡发送数据并接收来自微波电子卡的应答信号，它包括数字电路模块、射频电路模块和天线；数字电路模块又包括控制部分和数据解调部分，射频电路模块调制发射到防伪微波电子卡的数据，提供一个连续载波用于微波电子卡的反向散射波，接收和解调来自防伪微波电子卡的反向散射波信号；快速检索辅助单元主要由单片机 MCU 组成，它与读写检测单元相连，对读写检测单元读入的数据进行分析处理。

所述方法是利用上述车辆防伪微波电子卡和车辆防伪微波电子卡检测系统进行车辆防伪的，其特征是包括以下步骤：1）将微波电子卡初始化及个人化，包括由交管部门向车辆防伪微波电子卡中写入下述几种信息：车辆国际终身编码、车主身份证号、车牌号、发动机号、车架号、车型、识别代码；2）初始化及个人化的微波电子卡连同车牌一起发给车主，作为车辆入户认证的电子身份证；3）将微波电子卡安装于车辆上。

由于采用了以上的方案，将机动车辆关键性的物理数据及特征通过计算机技术写入一个智能化的电子媒体，称之为“车辆防伪微波电子卡”。实际上它是作为车辆的电子身份证，在车辆上牌入户时，由交管部门车管所连同车牌一起发给车主。车牌较易伪造，但微波电子卡内由于采用了微电子技术、计算机技术等现代科技手段，且易于对数据进行加密技术处理，保证了微波电子卡的唯一性和不可伪造性。微波电子卡的使用同交管部门管理体制和管理方法相结合，在一定程度上可以从车

辆的买赃卖赃、黑市交易、某些执法人员的贪赃枉法等源头上予以遏制，从而减少由于因盗抢车辆谋利的诱惑而演生的犯罪率。从这一点上讲，防伪微波电子卡同车牌一样都是车辆合法性入户认证的根本依据，也是交管执法人员检查车辆合法性或非法性的基本档案。另外，即使社会上发生车辆被盗抢的犯罪活动，由于本系统采用微波技术，执法人员也能在不停车的情况下在较远距离（15 米），用最短的时间和简便的操作方式，即以检测如<车辆国际终身编码>等最关键信息的真伪来及时分辨被查车辆的合法性、或非法性，便于交管人员采取相应的处理措施，从这一点上来讲，防伪微波电子卡又提供了执法人员固定检测和随机检测的方便性、机动性和可靠性。

图 1 是本发明车辆防伪微波电子卡功能方框示意图。

图 2 是本发明微波电子卡检测系统读写检测单元功能方框示意图。

图 3 是本发明微波电子卡形成流程图。

图 4 是固定式检测流程图。

图 5 是车辆被截停后人工处理流程图。

图 6 是机动式随机检测流程图。

下面通过具体的实施例并结合附图对本发明作进一步详细的描述。

实施例一：为了完整描述，本实施例同时包括了一种车辆防伪微波电子卡、微波电子卡的检测系统及基于此微波电子卡和检测系统的车辆防伪检测方法。其中：

所述车辆防伪微波电子卡包括有处理器 CPU、只读存储器 ROM、动态存储器 RAM、微波发射机、微波接收机、唤醒时间器、标识符识别区；每一个微波电子卡的标识符识别区中有一个芯片的出厂唯一编号；所述动态存储器 RAM 中存储有下述各种代码：<车辆国际终身编码>、<车主身份证号>、<车牌号>、<发动机号>、<车架号>、<车型>、<识别代码>；所述只读存储器 ROM 中存储有芯片管理系统 COS，即监控程序，管理上

述动态存储器 RAM 中的信息的读或不能读、写或不能写、改或不能改；微波发射机、接收机用于与外界设备进行连接，向微波电子卡中写入数据或读出微波电子卡中的数据；唤醒时间器用于控制微波电子卡的“休眠”与工作状态转换。微波电子卡内还设置有数据自毁终端，在遇破坏或被强行取走时，存储数据自动消失。

所述车辆防伪微波电子卡检测系统，包括读写检测单元、快速检索辅助单元；其中读写检测单元用于向防伪微波电子卡发送数据并接收来自防伪标识牌的应答信号，它包括数字电路模快、射频电路模块和天线；数字电路模块又包括控制部分和数据解调部分，射频电路模块调制发射到微波电子卡的数据，提供一个连续载波用于防伪微波电子卡的反向散射波，接收和解调来自防伪微波电子卡的反向散射波信号；快速检索辅助单元主要由单片机 MCU 组成，它与读写检测单元相连，对读写检测单元读入的数据进行分析处理。还包括有系统微机，它与读写检测单元的连接是通过快速检索辅助单元，它与快速检索辅助单元中的单片机 MCU 之间采用高速双口 RAM 以并行方式传送数据，并可以采集、存储、比对、分析、处理车辆微波电子卡的有关信息；它还通过网络连接公安部交管局各省、市车辆管理所的局域网上，上传、存放、下载各种车辆专用信息；微机中还存有疑点车辆数据库；可以按比对检测结果发出截停或放行车辆的指令。根据需要，本检测系统可以分为三种，一种是固定式，设置于道口、收费站等处，系统中设置有数字式车辆检测器、自动道闸和电子眼；数字式车辆检测器采用数模转化技术，通过电磁感应原理，感应检测并计数通行车辆；自动道闸用于拦截疑点车辆；电子眼用于对车辆进行摄像。另一种是移动式，所述微机为手提式电脑，通过无线调制解调器上网。第三种是手持式。

所述车辆防伪方法是利用上述车辆防伪微波电子卡和车辆防伪微波电子卡检测系统进行车辆防伪的，其特征是包括以下步骤：1）将微波

电子卡初始化及个人化，包括由交管部门向车辆防伪微波电子卡中写入下述几种信息：车辆国际终生编码、车主身份证号、车牌号、发动机号、车架号、车型、识别代码；2）初始化及个人化的微波电子连同车牌一起发给车主，作为车辆入户认证的电子身份证；3）将微波电子卡安装于车辆上。在对微波电子卡进行初始化及个人化时，还将下述几种信息的至少二种进行押码加密处理，然后将加密后的信息一并写入微波电子卡中：<车辆国际终身编码>、<车主身份证号>、<车牌号>皆须进行押码处理；发动机号、车架号、车型、识别代码不用进行押码处理。根据固定式和移动式的不同，其用法也不同。在主干道、检查站、道桥关口等处设置固定式车辆防伪微波电子卡检测系统，在不停车的情况下对过往车辆进行逐一检查或随机检查；快速检索辅助单元通过检测单元利用微波信号即时读取被检车辆上的微波电子卡电内的数据，传送到系统微机，系统微机对数据进行处理，决定放行或截停车辆。在巡查车上设置移动式车辆防伪微波电子卡检测系统，对过往车辆进行人机相结合的随机检查，快速检索辅助单元通过检测单元利用微波信号即时读取被检车辆上的确电子标识牌内的数据，传送到系统微机，系统微机对数据进行处理，决定放行或截停车辆。执勤者持手持式车辆防伪微波电子卡检测系统，对过往车辆或停泊车辆进行人机相结合的随机检查，快速检索检测系统<疑点车辆数据库>，决定放行或截停、扣押车辆。

下面对本实施例的各部分进一步详述。

一、 本实施例车辆防伪微波电子卡及检测系统的构成

本系统由以下几部份构成：

（一）、作为车辆防伪微波电子卡的微波电子芯片为达到较远距离（15米）不停车检测车辆的合法性或非法性的技术要求，采用了 2.45GHZ

载波频率的微波识别硬件框架。主要技术参数是：带八位 CPU； 有 4K 字节 ROM； 有内部 256 字节 RAM； 有用户 256 字节 RAM； 功率：300mw； 检测距离：15 米； 可以不停车检测时速为 100 公里的过往车辆； 读/写检测单元对微波电子卡芯片的正向链接的数据传输速率：189Kbps； 微波电子卡芯片对读/写检测单元的反向链接的数据传输速率：92Kbps； 使用环境温度：-40℃~+85℃。其功能方块图见图 1。

（二）、作为在较远距离（15 米）向微波电子卡发送数据信号及接收来自防伪微波电子卡应答信号的读/写检测单元。

检测单元由数字电路模块和射频电路模块两部分组成，数字电路模块又由控制部分和数据解调部分组成。射频电路模块完成调制发射到防伪微波电子卡芯片的数据，完成提供一个连续载波用于微波电子卡的反向散射波，完成接收和解调来自防伪微波电子卡芯片的反向散射波信号。其主要技术参数是：

1. 正向链接

主时钟频率：19.075MHZ； 数据速率：307.66bps （有效 189.33Kbps）；频率：2422MHZ； 调制：已滤波 OOK； 发射功率：最大 500mw（+27 毫瓦分贝）； 直接时序传播频谱：每位 31 分割， 分割速率：9.537 兆周/秒； 代码长度：31； 错误校正/检测：16 位检验和，5 位奇偶校验（一位校正，二位检测）； 解调技术：二极管检波器。

2. 反向链接

数据速率：149bps(有效 91.75Kbps)； 频段：低段 2418MHZ（±

15MHZ)、中段 2442MHZ（±15MHZ)、高段 2465MHZ（±15MHZ） 调制：反向散射波用差分相移键控副载波； 副载波频率：596KHZ； 频率跳跃：每段 75 次数，间隔 400KHZ； 跳跃速率：每个信息一次； 信息长度；变换高度 104 字节；接收灵敏度：最小-80 毫瓦分贝； 副载波调解：用 DSP 差分相移键控； 错误校正：16 位校验和，5 位奇偶检验（一位校正，二位检测)； 交错：每个数据字对是交错的。其功能方块图见图 2。

（三)、双发射天线和双接收天线

两个发射天线和两个接收天线；发射天线是 6dp 的补偿天线，接收天线是 12dp，由于增益不同，接收天线的尺寸仅为发射天线的 1/3。

（四)、快速检索辅助单元

单片机电路组成

连接于读/写检测单元和系统主机之间，主要负责监控读卡，减轻系统微机的负担，提高系统微机查找相关数据的速度，辅助单元的 MCU 同系统之间采用高速“双口 RAM”以并行方式传送数据。辅助单元有以下功能：

①有车辆通过时，“数字式车辆检测器”将车辆通过信号通知辅助单元，得知过往车数，单元的 MCU 读取设定车道上通行车辆上的微波电子卡数据。

②单元的 MCU 读不到设定车道上通行车辆微波电子卡的数据时，说明该车辆无微波电子卡或已坏，及时通知系统微机下令截停该车查询。

③辅助单元的 MCU 首先读取并校验微波电子卡内的“微波电子卡序列索引编号”，并将信息及时传送到系统微机；单元 MCU 则继续读取<车辆国际终身编码>等数据，“微波电子卡索引编号”可以利用交管部门现有某些索引编号的数字，如国家、省、市代码，加上发行微波电子卡芯片时的序列号组成。

④系统微机收到来自单元 MCU 的“微波电子卡序列索引号”后，即按索引号在有关数据库中查找相关信息，并等待同单元 MCU 联系核对数据。

⑤单元 MCU 读出的<车辆国际终身编码>将微波电子卡在发卡时已加密生成的<车辆国际终身编码>的原押码同新读出的 26 字节的<车辆国际终身编码>和 6 字节的出厂唯一编号再同 8 字节的“机站密钥”通过 SHF 加密算法后得出的新的押码进行比对，如吻合则属正确，通知系统微机下令放行。如属错误即刻将信息传送到系统微机做进一步处理。

⑥系统微机将单元 MCU 送来的“错误”信息在疑点车辆数据库中比对，

从而查出是否已报警的盗抢、遗失、走私车辆。

⑦判定非法车辆除主要根据<车辆国际终身编码>信息外，截停疑点车后，还可以从另一联网的系统微机通过交管局网络服务器从各省市车管所数据库调查其它所需的数据资料，如车主身份证号码、车牌号、发动机号、车架号、车型、识别代号等。

（五）、微波电子卡芯片初始化及个人化的发卡系统

发卡系统由发卡机和发卡系统软件组成，发卡时由授权卡授权开机。初始化及个人化的发卡系统软件包括根据卡号生成的“微波电子卡序列索引编号”，发行用户微波电子卡及管理软件；数据查询（用户微波电子卡浏览、管理卡浏览、核对查询）软件；下装数据软件；疑点车辆数据处理（疑点车辆数据录入、生成数据文件、数据查询）软件；系统功能（配置系统参数、注销、退出系统）软件。

（六）系统微机主机及微机

1. 连接公安部交管局各省、市车辆管理所的局域网上，上传、存放、下载各种车辆专用信息。

2. 采集、存储、比对、分析、处理车辆微波电子卡内的有关部门信息。

3. 存放“疑点车辆数据库”

4. 按检测结果，命令截查机构放行合法车辆，或命令截查机构截停非法车辆。

5. 系统微机分为主机和副机各一台，主机用于日常检测过往车辆；副机用于核对被截停查车辆的各种信息数据，副机连接公安部交管局广域网，并通过广域网服务器调用其它省、市车管所车辆标准数据库的数据以备查询。

（七）、数字式车辆检测器和自动道闸

数字式车辆检测仪包括信号处理器和检测线圈两个部分。

采用了先进的数模转化技术，通过电磁感应原理，在 30KHZ 到 180KHZ

感应范围检测并计数通行车辆。

检测仪技术参数：

计数误差，1×10^{-6}；交直流：12~20V, +50HZ； 感应范围：30KHZ~180 KHZ； 输出信号：感应时电平信号，离开时脉冲信号。 RS-485 接口； 检测线圈采用 1mm 单芯铜芯 BVC 塑料线，长度 100mm，均匀绕置于线槽内，出口处以双线绕线引出。槽内全部用环氧树脂封罐好。技术参数：导线：O 1mm×100 m；线圈电阻小于 4Ω；线圈面积：2.5m×1.5m;线圈对地绝缘电阻：10MΩ；自动道闸：全自动式，传动结构简单，减速机选用标准摆线针轮减速机，体积小、传动比大、效率高，停电时可用于手柄转动闸杆。内设控制器，根据系统微机发来的启落信号进行启落操作，启动迅速只需 2 秒。技术参数：电源：220V~50HZ 单相；主机功耗：180W n=1450r、p、m：功率：最大限度 130W；接口方式：输入开关电平：直流 10~15V, 10MA； 输出方式有可控硅和继电器两种；闸杆升起（降落）时间 t=2 秒；噪音：<70 分贝；重量：60KG。

二、工作原理

（一）、微波电子卡的形成

其流程图如图 3。由交管部门省市地区交管所应用微波电子卡发卡系统向微波电子卡芯片内写入：

1. 4 字节（暂定为 4 字节）的“微波电子卡序列索引编号”（放在 10 个字节标识符识别区的后 4 个字节用户识别区内）

2. 读/写检测单元和快速检索辅助单元一次性读取 10 字节的标识

符识别区，先读 6 字节的芯片出厂唯一编号，再读 4 字节的微波电子卡序列索引编号。

3. 向芯片内的 256 字节 RAM 区内写入标识牌的最关键的<车辆国际终身编码>信息，在写入车主身份证号码、车牌号、发动机号、车架号、车型、识别代号等信息。

4. “车辆国际终身编码”、“车主身份证号码”、“车牌号”三个主要信息需要进行押码加密处理，使之不可能做到伪造。

5. 芯片内的 8 位 MCU 和 ROM 区内存放的监控程序（COS）严格管理各种信息的读或不能读，写或不能写，改或不能改，保证了微波电子卡信息的读取更改及存储的安全性。

6. 芯片内 256 字节的用户 RAM 区尚余留 122 字节的存储空间，作为日后发展所需，如车辆肇事记录及电子钱包等用途。

7. 初始化及个人化后的微波电子卡连同车牌一起发给车主，作为车辆入户认证不可能伪造的车辆电子身份证。

（二）、微波电子卡的安装

1. 微波电子卡（约 80×50mm）应同车辆一起安装，卡不离车，车不离卡.

2. 微波电子卡安装在车头挡风玻璃内上方。

3. 微波电子卡应用有机溶剂将微波电子卡同挡风玻璃溶接为一体。

4. 微波电子卡表面按交管部门规定印有有关部图案及相关标志。

5. 为保证微波电子卡车辆一体化，在系统工程正式启动后，可要求芯片制造厂家在芯片内设置数据自毁端，即遇破坏标识牌或强行取走微波电子卡时卡内的存储器数据会自动消失。

（三）、交管部门车管所配备有微波电子卡发卡系统、微波电子卡读/写检测单元和快速检索辅助单元以便及时处理发卡、查卡、坏卡处理、丢卡备案、车辆年检验卡等业务事项。

（四）、车辆的网点检测和随机检测有两种方式进行。一种是固定式检测：即在主干道、检查站、道桥关口等处设定固定式检测点；固定式检测点配置有系统微机（主辅）、读/写检测单元、快速检索辅助、单元数字式车辆检测器、自动道闸、电子眼等设备。另一种是机动性随机检测方式，即在巡查车上配置手提电脑式系统微机、读/写检测单元和快速检索辅助单元、无线调制解调器、电源逆变器等。

（五）、检测微波电子卡信息时，可在距天线 15M 范围，90 度角内检测时速为 100 公里的过往车辆，同时可检测到 20 辆车的微波电子卡信息。

（六）固定式检测方式检测：其流程图见图 4，其中截停后的处理程序见图 5。

1. 数字式车辆检测器及时将过某车道检测段的车辆信号传送到系统微机，以便确定在某时段过往车辆的数量，防止无微波电子卡的车辆漏检。

2. 快速检索辅助单元即刻读取车辆微波电子卡内的 10 字节标识符

ID 区，先读 6 字节的微波电子卡芯片厂唯一编号，再读 4 字节的车辆索引编号，并将信息传送到系统微机。

3.“辅助单元”继续读取微波电子卡芯片内的<车辆国际终身编码>。

4.“辅助单元”首先将<车辆国际终身编码>的原有加密押码同新的验证押码进行比对。即将<车辆国际终身编码>再同已读取的芯片的 6 个字节的出厂唯一编号，再同 8 字节“机站密钥”通过 SHF 加密算法得出后的新的押码进行对比。

5. 如比对结果相符，则通知系统微机对被检测的车辆放行。

6. 如比对结果不相符，则即将信息传至系统微机，再同系统微机中存放的“疑点车辆数据库”进行比对，找出是否是已报案的被盗抢和遗失或走私车辆。

7. 系统微机中的“疑点车辆数据库”存放的是全国被盗抢、遗失、走私车辆的统报数据及资料。由公安部交管局中西数据库按时通过网络向各省、市车管所传播，并能自动增、删、改写。

8. 固定检测点的系统微机是作为省、市车管所局域网的一个终端机，通过有线调制解调器由车管所主机下载加密的疑点车辆数据及资料到固定检测点的系统微机内，建立<疑点车辆数据库>。

9. 如比对结果，判定被检测车辆非法，则系统微机下令设置在离车道检测段 300 米处的自动道闸实行截停。

10. 被截停的车辆如执法人员需查询该车更多的信息，可以用另一台联网的微机通过交管局广域网服务器调用全国各省市车管所数据库

的有关其他信息，以便作出处理。

11. 如在同一时间内，数字式车辆检测器送出的车辆的数目信息同辅助单元检测到的微波电子卡信息一致，则证明过往车辆上都装有微波电子卡，如数目不符，则证明某些过往车辆上没有装微波电子卡，对于无微波电子卡车辆，系统微机即下令截停处理。

（七）、机动车随机检测方式，其流程图见图 6。

机动检测方式须结合固定式检测方式才能取得较好的效果，从某些意义上讲，机动车随机检测可能还会取得更好的效果。巡查车上配备读/写检测单元和快速检索辅助单元、手提式电脑、无线调制解调器、电源逆变器等，并有专人负责。实行人机结合检测，手提式电脑内建有疑点车辆数据库，可以事先下载，也可以通过无线调制解调器实时下载或实时增删、更改。机动式检测主要对流动车辆，也对停止车辆进行随机检测；检测结果除由机器得出判断外，也由人的观察、分析得出判断，如检查人员发现从某车微波电子卡内取得的<车辆国际终身编码>“车型”“车牌号”数据同实际观察到的“车型”“车牌号”不符，即可截停车做进一步查询处理，车载系统微机也可以通过无线调制解调器方式租用 GSM 信道同交管局广域网络联接，对截停车辆复查时，并可通过交管局广域网络服务器调查各省、市车管所数据库的车辆有关部门数据和资料。根据需要也可采用手持式微波读/写设备进行机动式随机检查。

三、本实施例车辆防伪微波电子卡、检测系统的安全性设计

检测系统的安全性涉及微波电子卡芯片、读/写检测单元、系统微

机、发卡系统及网络传输。

（一）、特别要求安全性高的是微波电子卡芯片，现有以下几种措施予以保证：1）芯片结构带有 8 位 MCU 及 4K 字节的 ROM 区。通过 MCU 的安全管理机制及 ROM 区内有效的监控程序（COS）严格控制存储区内数据的可读或不能读，写或不能写，改或不能改。2）6 个字节不可改写的 ID 区，存放出厂唯一芯片编号，保证了 43 亿分之一以上的唯一性。3）预留 26 个字节的<车辆国际终身编码>同 6 个字节的“芯片唯一编号”，加上 8 个字节的“机站密钥通过不可逆的保密押码函数 SHF 算法得出一个高安全性的 6 字节押码。由于保密押码函数是一个单向函数，即已知 x，求 y=f（x）很容易，反过来已知 y，求 x 则不可估算，保证了它的不可逆性。保密押码函数还具有良好的随机性，如输入全 0，输出非全 0，且输出中 0 和 1 的个数接近；输入全 1，输出非全 1，且输出中 0 和 1 的个数接近；任意改变输入中 1 位，输出的变化位数将达到总位数的一半左右。由于不可逆性和随机性，企图伪造押码几乎是不可能的。实践证明，保密押码函数计算产生一次押码仅需 3。3ms，并且总的程序量小于 1K 字节。

（二）、读/写检测单元和系统安全性要同交管业务部门的严格管理制度相结合。要有系统操作管理授权及执勤操作授权。如果需要将传输数据加密，以密文形式传输到标识牌芯片内，可以在读/写检测单元内加入硬件形式“加密控制器 IC”。如具有基于非对称算法，16 位 CPU，1100 为算法加密协处理，写/擦除时间为 1.8~3.6ms，型号为 SLE66CX80S

的加密控制器。也可以应用滚动加密将数据加密后传输到标识牌芯片内，滚动加密法具有将一位信息可以加密到任意数，不可逆转，一对一加（解）密密钥，密钥可以从四位到几十位到几百位等特性。

（三）、发卡系统的安全性特别要同交管业务部门的管理体制和管理制度相结合。严格实行管理授权及格操作授权互相制约的方法。

（四）、网络传输的安全性基本上根据交管部门的实际网络和局部网络的安全规范进行操作。要强调网络传输的授权管理，关键数据的加密管理和三级动态密钥管理。

（五）、系统微机同交管业务部门的网络接口，按规范化的网络传输标准和接口标准衔接。

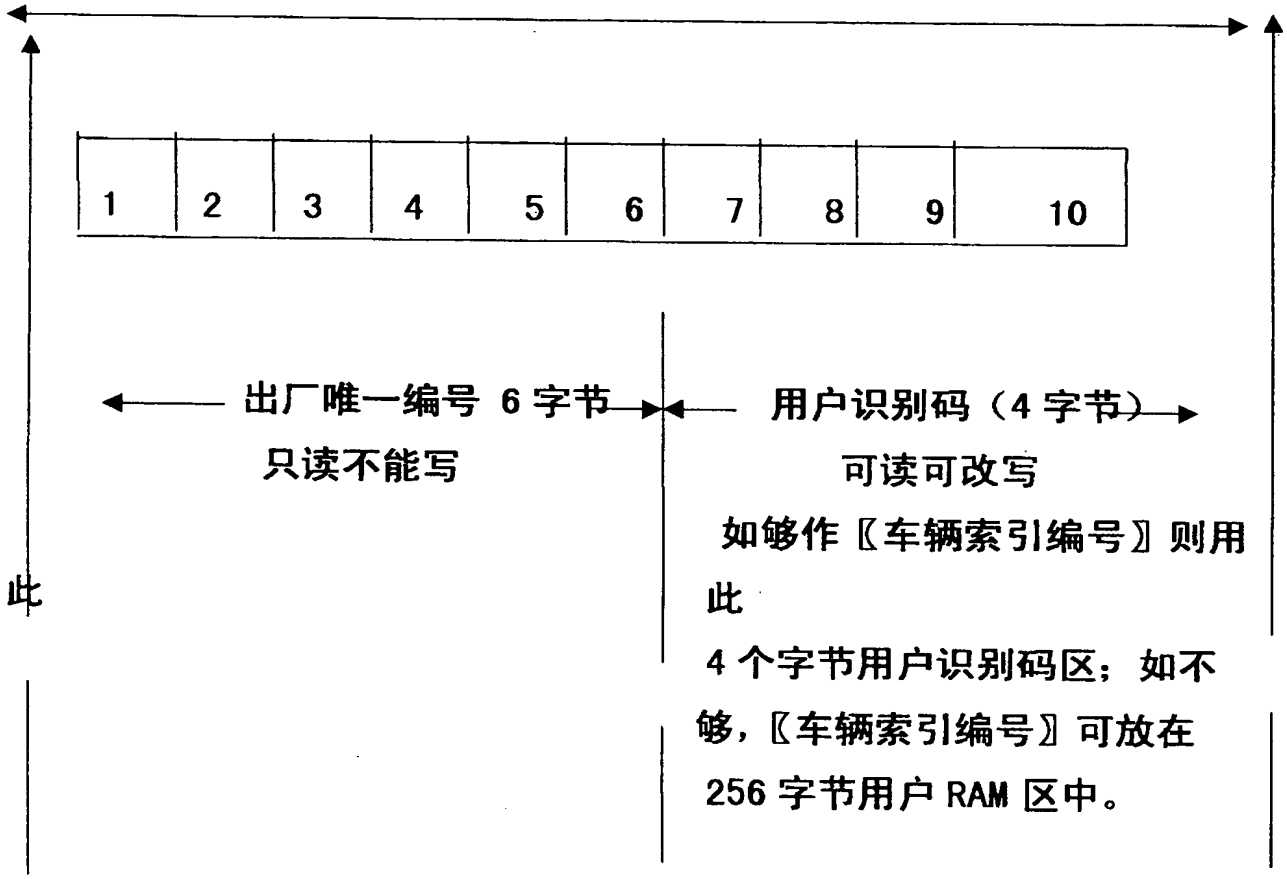
表一列出了本实施例车辆防伪微波电子卡芯片储存信息的资源分配；表二列出了微波电脑芯片内 10 个字节的标识符识别区的情况。

01.01.20

表一：芯片储存信息的资源分配

编号	信息名称	数据形式	字节数	地 址	其 它
1	首标志	固定	1B	00H	M
	车辆国际终身编码	任意	26B	01-18H	汉字小于五位. 英文小于五位. 数字,
	押码	任意	6B	19-1CH	计算产生
	尾标志	固定	1B	1DH	K
2	车主身份证	数值	10B	1E-27H	压缩 BCD 码（实长：20 字符）——→
	押码	任意	6B	28-2DH	计算产生
3	车牌号	任意	10B	2E-37H	由汉字、英文、数字组成
	押码	任意	6B	38-3DH	计算产生
4	发动机号	ASCII	21B	3E-52H	由 21 个英文，数字组成
5	车架号	任意	23B	53-69H	由 21 个汉字、英文，数字组成
6	识别代号	任意	17B	6A-7AH	任意字符
7	车型	汉字	10B	7B-84H	1-5 个汉字
	剩余空间		122B	85-FFH	根据发展需要可留作一卡多用

表二：微波电脑芯片内 10 个字节的标识符识别区



说 明 书 附 图

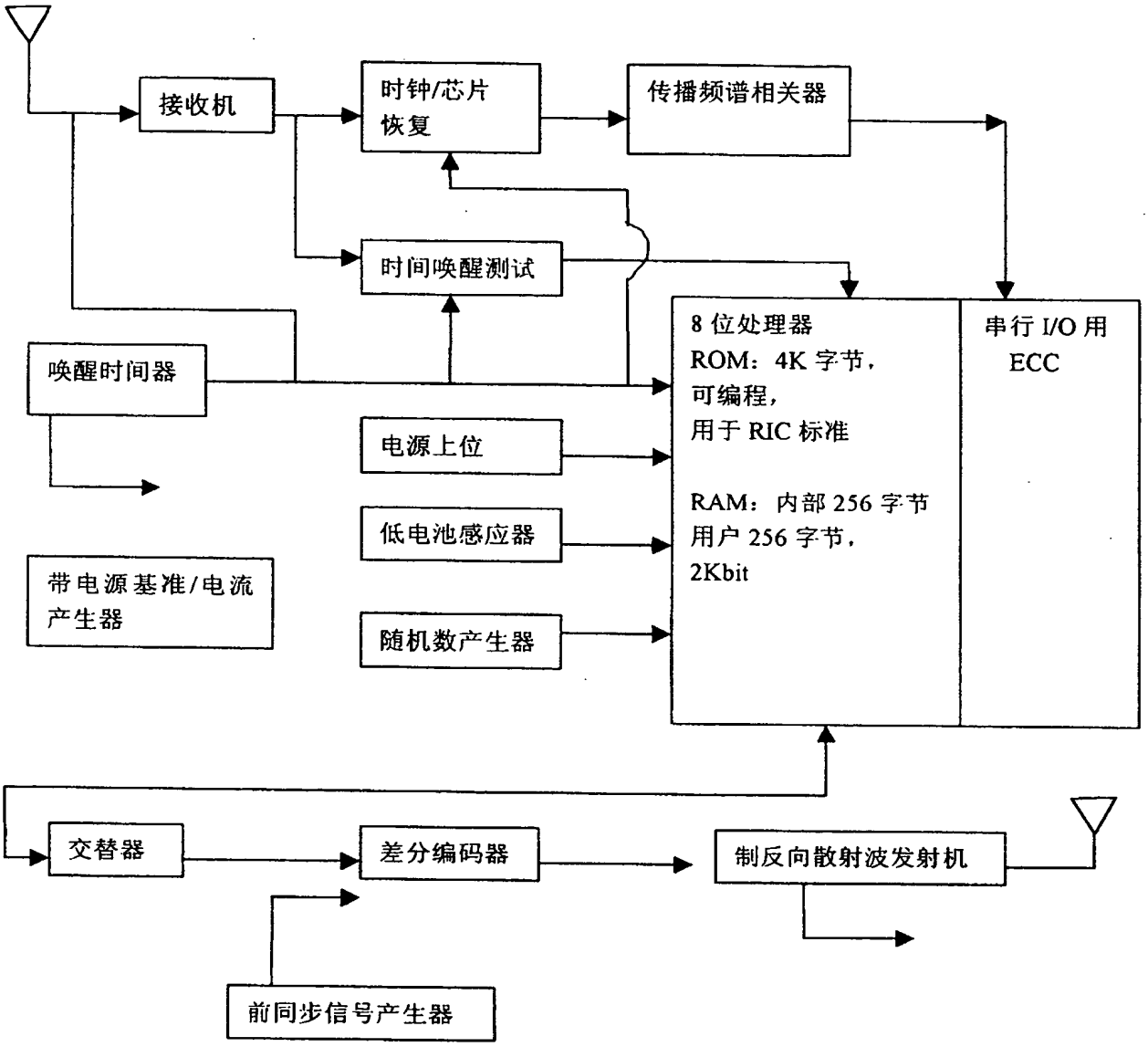

接收机
时钟/芯片
恢复
传播频谱相关器
时间唤醒测试
唤醒时间器
8 位处理器
ROM：4K 字节，
可编程，
用于 RIC 标准
RAM：内部 256 字节
用户 256 字节，
2Kbit
串行 I/O 用
ECC
电源上位
低电池感应器
带电源基准/电流
产生器
随机数产生器
交替器
差分编码器
制反向散射波发射机
前同步信号产生器

图 1

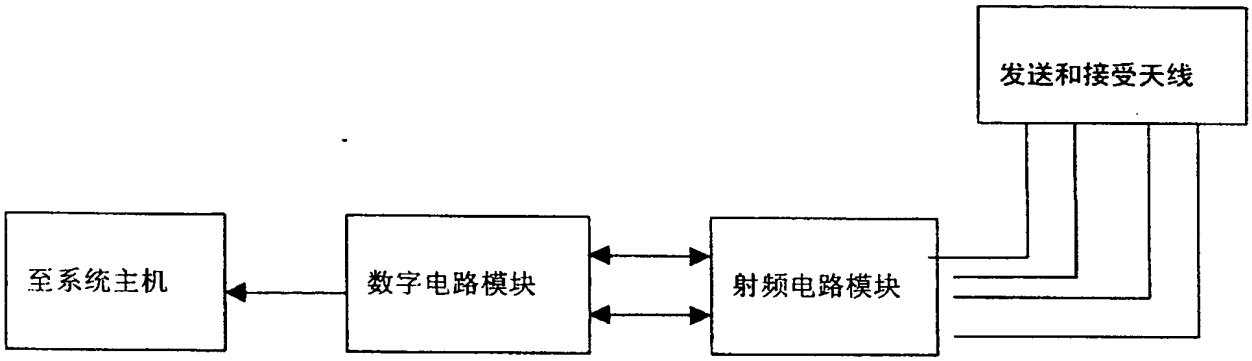


图 2

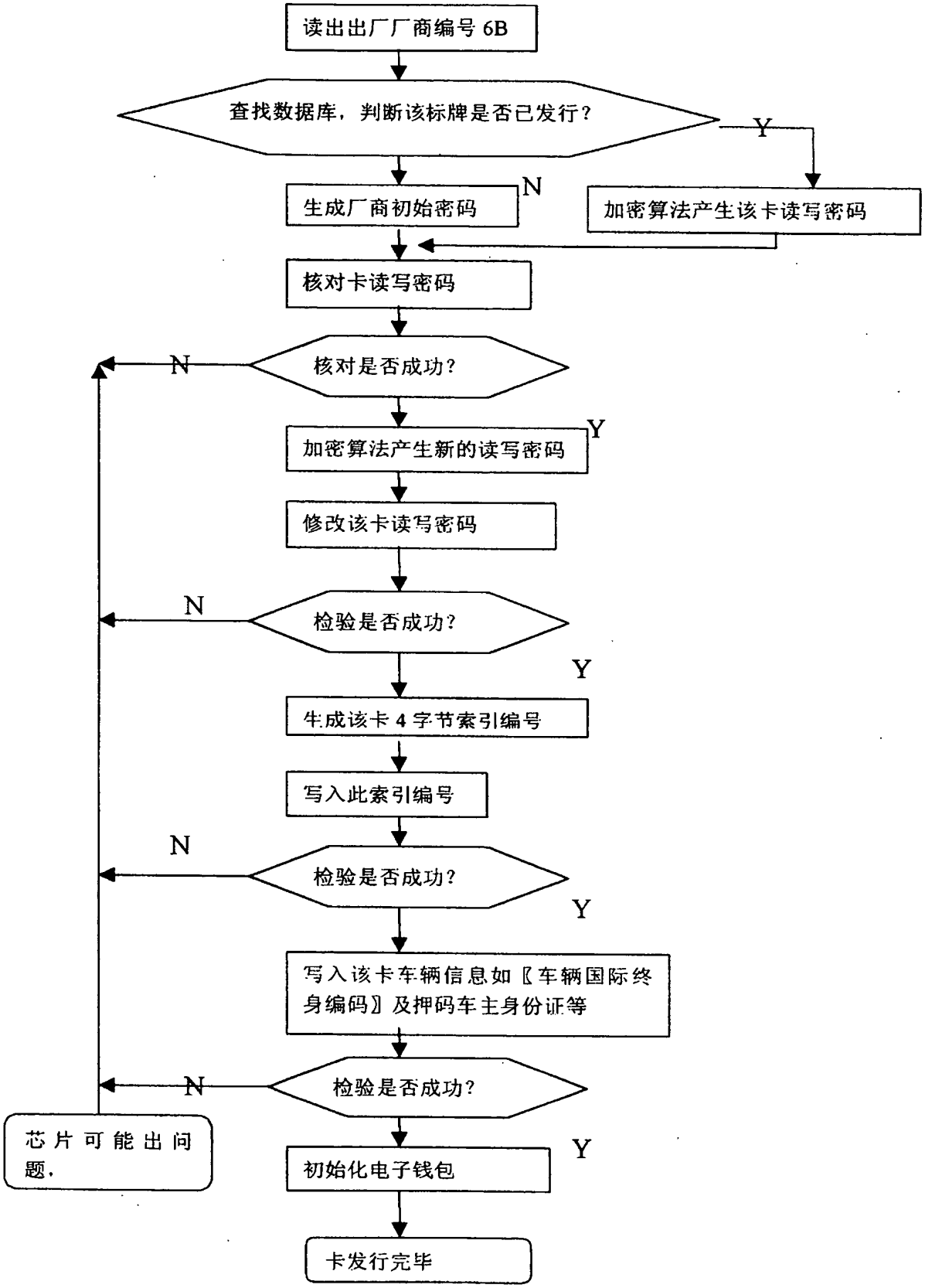

读出出厂厂商编号 6B
查找数据库，判断该标牌是否已发行？
Y
N
生成厂商初始密码
加密算法产生该卡读写密码
核对卡读写密码
核对是否成功？
N
Y
加密算法产生新的读写密码
修改该卡读写密码
检验是否成功？
N
Y
生成该卡 4 字节索引编号
写入此索引编号
检验是否成功？
N
Y
写入该卡车辆信息如〖车辆国际终身编码〗及押码车主身份证等
检验是否成功？
N
Y
芯片可能出问题，
初始化电子钱包
卡发行完毕

图 3

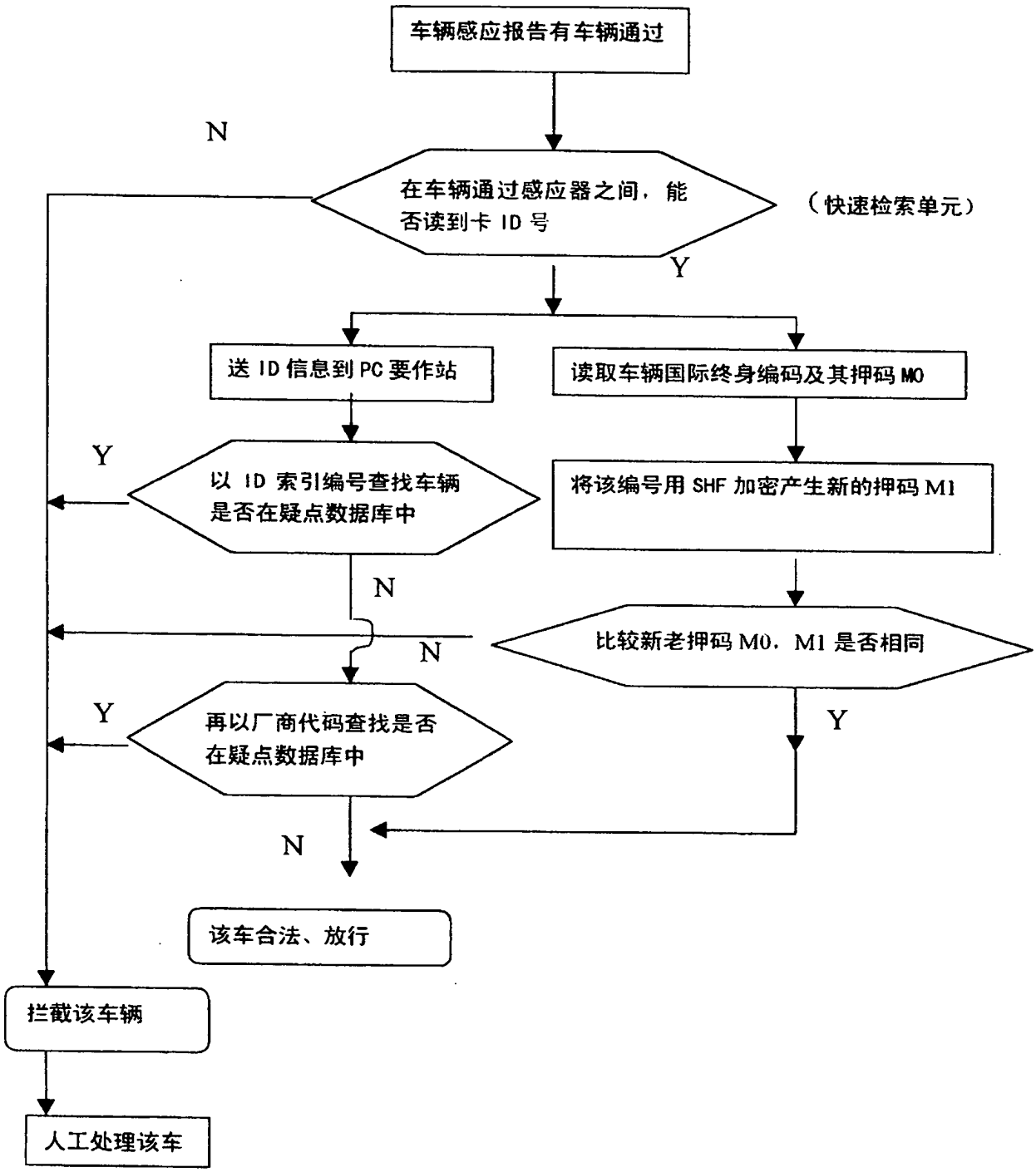

车辆感应报告有车辆通过
N
在车辆通过感应器之间，能否读到卡 ID 号
（快速检索单元）
Y
送 ID 信息到 PC 要作站
读取车辆国际终身编码及其押码 M0
Y
以 ID 索引编号查找车辆是否在疑点数据库中
将该编号用 SHF 加密产生新的押码 M1
N
N
比较新老押码 M0，M1 是否相同
Y
Y
再以厂商代码查找是否在疑点数据库中
N
该车合法、放行
拦截该车辆
人工处理该车

图 4

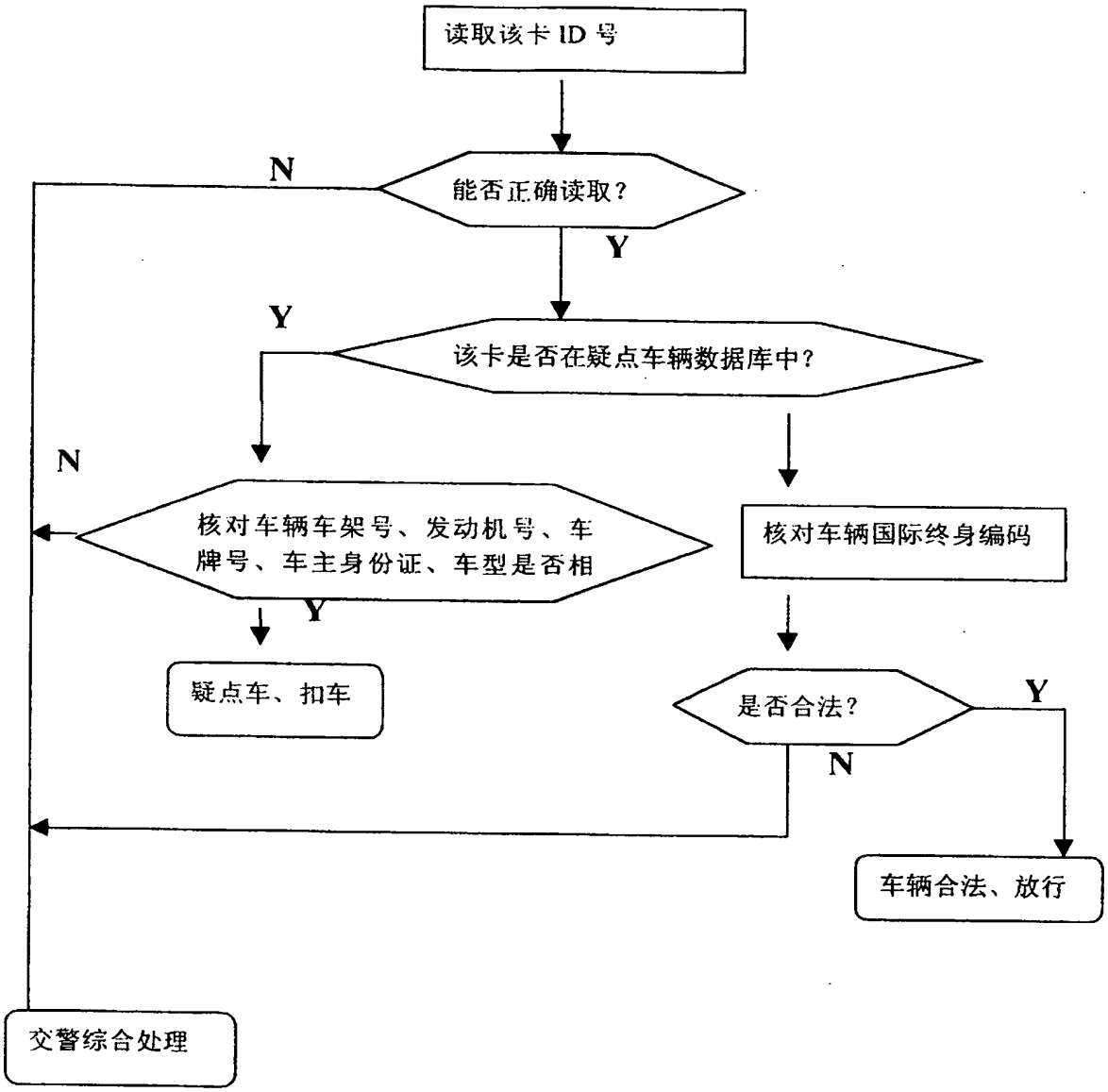

读取该卡 ID 号
能否正确读取？
N
Y
该卡是否在疑点车辆数据库中？
Y
N
核对车辆车架号、发动机号、车牌号、车主身份证、车型是否相
Y
核对车辆国际终身编码
疑点车、扣车
是否合法？
Y
N
车辆合法、放行
交警综合处理

图 5

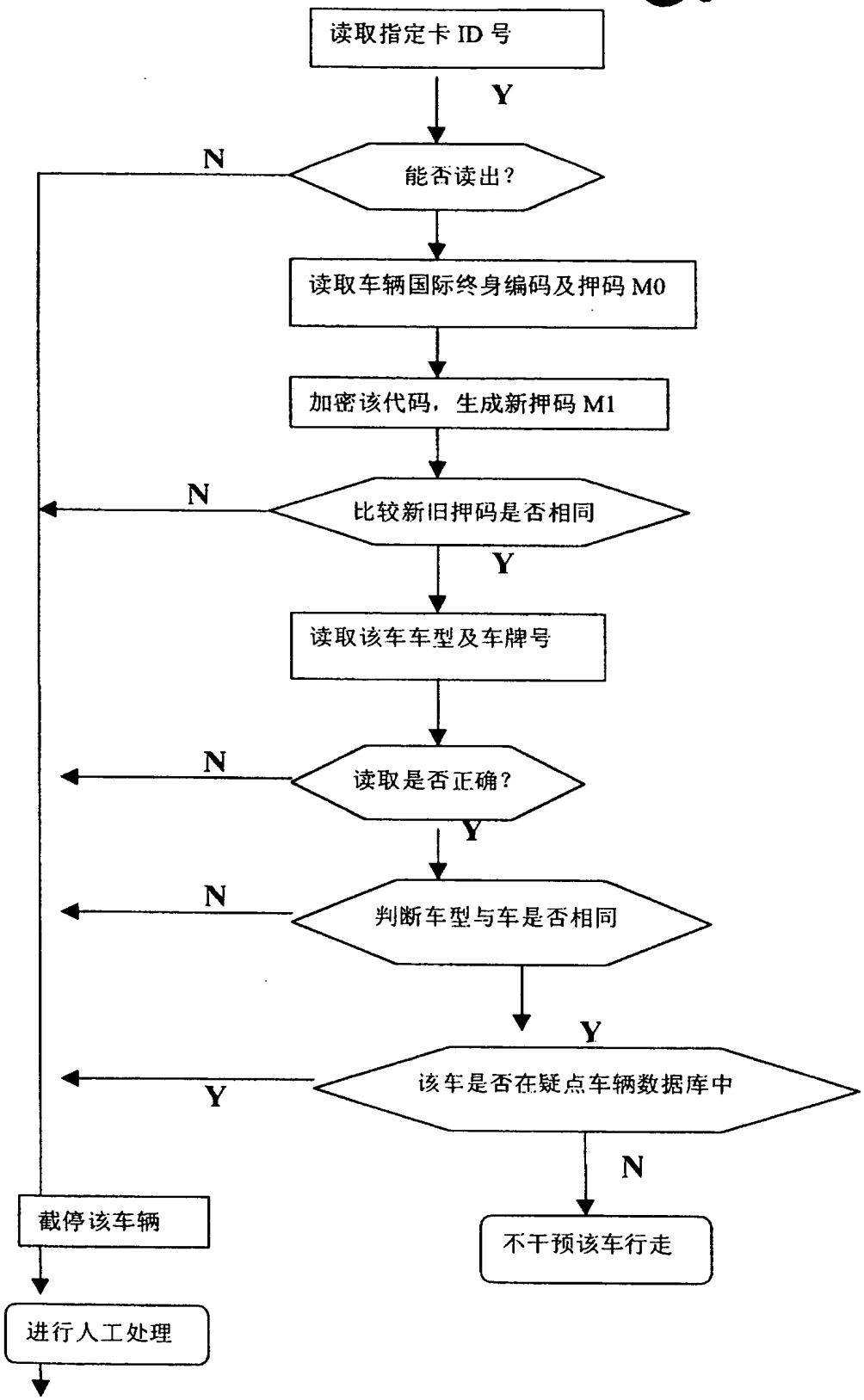

读取指定卡 ID 号
Y
N
能否读出？
读取车辆国际终身编码及押码 M0
加密该代码，生成新押码 M1
N
比较新旧押码是否相同
Y
读取该车车型及车牌号
N
读取是否正确？
Y
N
判断车型与车是否相同
Y
Y
该车是否在疑点车辆数据库中
N
截停该车辆
不干预该车行走
进行人工处理

图 6